

Commonwealth Office of Technology Monthly Cyber Security Tips

JULY 2006

Volume 1, Issue 2

How Anonymous Are You?

From the Desk of the Chief Information Security Officer

What information is collected?

When you visit a web site, a certain amount of information is automatically sent to the site. This information may include the following:

- **IP address** - Each computer on the internet is assigned a specific, unique IP (internet protocol) address. Your computer may have a static IP address or a dynamic IP address. If you have a static IP address, it never changes. However, some ISPs own a block of addresses and assign an open one each time you connect to the internet—this is a dynamic IP address. You can determine your computer's IP address at any given time by visiting www.showmyip.com.
- **domain name** - The internet is divided into domains, and every user's account is associated with one of those domains. You can identify the domain by looking at the end of URL; for example, .edu indicates an educational institution, .gov indicates a US government agency, .org refers to organization, .com is for commercial use. Many countries also have specific domain names. The list of active domain names is available at <http://www.iana.org/domain-names.htm> or <http://www.norid.no/domenenavnbaser/domreg.html>.
- **software details** - It may be possible for an organization to determine which browser, including the version, that you used to access its site. The organization may also be able to determine what operating system your computer is running.
- **page visits** - Information about which pages you visited, how long you stayed on a given page, and whether you came to the site from a search engine is often available to the organization operating the web site.

If a web site uses cookies, the organization may be able to collect even more information, such as your browsing patterns, which include other sites you've visited. If the site you're visiting is malicious, files on your computer, as well as passwords stored in the temporary memory, may be at risk.

How is this information used?

Generally, organizations use the information that is gathered automatically for legitimate purposes, such as generating statistics about their sites. By analyzing the statistics, the organizations can better understand the popularity of the site and which areas of content are being accessed the most. They may be able to use this information to modify the site to better support the behavior of the people visiting it.

Another way to apply information gathered about users is marketing. If the site uses cookies to determine other sites or pages you have visited, it may use this information to advertise certain products. The products may be on the same site or may be offered by partner sites.

However, some sites may collect your information for malicious purposes. If attackers are able to access files, passwords, or personal information on your computer, they may be able to use this data to their advantage. The attackers may be able to steal your identity, using and abusing your personal information for financial gain. A common practice is for attackers to use this type of information once or twice, then sell or trade it to other people. The attackers profit from the sale or trade, and increasing the number of transactions makes it more difficult to trace any activity back to them. The attackers may also alter the security settings on your computer so that they can access and use your computer for other malicious activity.

Are you exposing any other personal information?

While using cookies may be one method for gathering information, the easiest way for attackers to get access to personal information is to ask for it. By representing a malicious site as a legitimate one, attackers may be able to convince you to give them your address, credit card information, social security number, or other personal data (see [Avoiding Social Engineering and Phishing Attacks](#) for more information).

How can you limit the amount of information collected about you?

- **Be careful supplying personal information** - Unless you trust a site, don't give your address, password, or credit card information. Look for indications that the site uses SSL to encrypt your information (see [Protecting Your Privacy](#) for more information). Although some sites require you to supply your social security number (e.g., sites associated with financial transactions such as loans or credit cards), be especially wary of providing this information online.
- **Limit cookies** - If an attacker can access your computer, he or she may be able to find personal data stored in cookies. You may not realize the extent of the information stored on your computer until it is too late. However, you can limit the use of cookies (see [Browsing Safely: Understanding Active Content and Cookies](#) for more information).
- **Browse safely** - Be careful which web sites you visit; if it seems suspicious, leave the site. Also make sure to take precautions by increasing your security settings (see [Evaluating Your Web Browser's Security Settings](#) for more information), keeping your virus definitions up to date (see [Understanding Anti-Virus Software](#) for more information), and scanning your computer for spyware (see [Recognizing and Avoiding Spyware](#) for more information).

This series of information security tips will give you more information about how to recognize and protect yourself from attacks.

For more information and this and other topics please visit the Commonwealth Office of Technology's Website at http://technology.ky.gov/security/cyber_security.htm

Brought
to you
by:



MS-ISAC

Powered
by:

<http://www.msisac.org>



<http://technology.ky.gov/>



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Copyright Carnegie Mellon University
Produced by US-CERT <http://www.us-cert.gov/>